Mandatory Reference - N/A
Supplementary Reference - 545
File Name - ads17/54553s5.doc

UNCLASSIFIED AUTOMATED INFORMATION SYSTEM COMPLIANCE REVIEW

This questionnaire was developed by M/IRM/IPA (security) for use as a guideline in assessing compliance with the Federal and USAID automated information systems security policies, procedures and regulations governing electronic data processing and storage.

The site ISSO, in conjunction with the Program Manager, System Manager/IT Specialist and other appropriate security personnel, shall use this questionnaire as a guideline for conducting an annual review of the security posture of each system operating in support of their mission or program. The completed questionnaire shall be retained, along with a plan for corrective action for all negative responses, in the central system file. A copy of the completed questionnaire and the associated plan for corrective action shall be forwarded to the "ISSO for USAID."

All questionnaire findings, supporting information and plans for corrective action may be used when M/IRM or the **Office of Security (**SEC**)** determines system certification, conducts system audits and inspections, and investigates security violations.

QUESTION	YES	NO
PERSONNEL SECURITY		
1. Do all members of the system staff and users with special access privileges meet the requirements for sensitive positions outlined in the ADS Security Chapter?		
2. Have all personnel accessing the system received, at a minimum, a favorable background check conducted by either SEC or the RSO?		
3. Have user access privileges been structured to reflect the separation of key duties?		
4. Have all rooms housing central processing units or servers been designated limited access areas?		
5. Is a visitors' log maintained of all personnel entering the computer/server room who do not have unescorted access privileges?		
6. Is an up to date "Authorized Access List" posted at or near the entrance to rooms housing the central processing units or servers?		
TECHNICAL SECURITY		
1. Is access to special system software, utilities and functionality that could be used to gain unauthorized access to application data and programming code limited to a minimum number of authorized users?		

2. Is all software operating on the system either approved by M/IRM/SDM for operation on the system or appropriately licensed to USAID for operation on USAID systems?		
3. Have operating system software and application software security controls been appropriately implemented?		
4. Is the system audit trail operational?		
5. Has the system audit trail been reviewed for anomalies and access violations on a regular basis?		
6. Are users restricted to specific workstations and printers on an individual basis?		
7. Are unsuccessful logon attempts restricted to three; and do keyboards lock out the user after three unsuccessful attempts?		
8. Are all users required to enter a unique user-ID to gain access to the system?		

QUESTION	**YES**	**NO**
9. Are passwords randomly selected and do they consist of at least six alphanumeric characters?		
10. Have passwords been changed within the last 90 days?		
11. Has the audit trail been archived and retained for at least 30 days?		
ADMINISTRATIVE SECURITY		
1. Have U.S. citizens with SECRET security clearances been formally appointed ISSO and alternate?		
2. Have all personnel accessing the system been formally granted system access privileges via the USAID Computer System Access & Termination Request form?		
3. Are all active user-IDs and passwords assigned to personnel currently working in the facility supported by the system?		
4. Have user access privileges been reviewed within the last 12 months?		
5. Have user-IDs and passwords supplied by the vendor resident on the system (e.g, IBMUSER, CSG, SYSTEM, FIELD, TEST) been deleted?		
6. Has the system and its associated storage media been browsed to ensure national security information is not being processed or stored on the system, and privacy information is being appropriately safeguarded?		
7. Is SBU information processed only on systems authorized for such purposes?		
8. Are all dial-in and network connections authorized and accounted for?		
9. Have system equipment and media used to process and store SBU information been appropriately labeled?		
10. Are SBU media appropriately stored?		

11. Have procedures for transporting system equipment and media been developed by the site ISSO and system manager/administrator?		
12. Is a log maintained of all requested and/or performed maintenance service?		
13. Is burning or shredding employed to destroy magnetic tape and floppy disks?		
14. Is there no classified national security information processed, printed or stored on the system?		
15. Is a central system file maintained and up-to-date?		
16. Are system data, file, and record backup procedures regularly implemented?		
17. Are up-to-date contingency operation plans in place?		
18. Have the contingency operation plans been successfully practiced or implemented within the last 12 months?		
19. Have up-to-date disaster recovery and emergency action plans been developed?		
20. Have the disaster recovery or emergency action plans been successfully practiced or implemented within the last 12 months?		
21. Have all system users received security awareness training within the last 12 months?		
22. Is a system operations log maintained?		
23. Has the system been formally approved to process SBU information?		
PHYSICAL SECURITY		
2. Is there a complete and up-to-date inventory of all system components and peripheral devices by location?		